VisionShare Testimony to the HIT Standards Committee:

Approaches to the Secure Transport of Healthcare Data

November 30, 2010
John Feikema, President

2829 University Ave SE Suite 800
Minneapolis, MN 55414
w: www.visionshareinc.com
p: 612.460.4301
f: 612.460.4343

Table of Contents

The VisionShare Approach 3
Principles 3
Security 4
Identity Verification 4
Addressability and Routability 4
Practicality and Simplicity of Integration 4
VisionShare and the Direct Project 5
High-Level Comparison 5
Security 5
Certificate Management 5
Backbone Protocol 6
Edge Protocols 6
Receipt Confirmation 7
VisionShare and CONNECT 7
Looking Back 8
Looking Forward 8

2829 University Ave SE Suite 800
Minneapolis, MN 55414
w: www.visionshareinc.com
p: 612.460.4301
f: 612.460.4343

Introduction

Thank you very much for the privilege of providing testimony to the HIT Standards Committee and guests. We are honored to be able to submit our thoughts and experiences regarding standards and approaches for secure point-to-point transport of health data.

We are very supportive of and pleased with the work of the Office of the National Coordinator (ONC) to help drive widespread adoption and meaningful use of electronic health records. In particular the Direct Project has been a notable step forward in this direction.

The VisionShare Approach

Principles

The VisionShare approach to building a successful secure healthcare communications network is founded on four key principles:

1. Utilize the ubiquity and affordability of the Internet to enable participation by players of all sizes.
2. Build Public Key Infrastructure (PKI) security technology into every facet of communication to ensure data P.A.I.N. (privacy, authentication, integrity, and non-repudiation).
3. Create bullet-proof, scalable business practices and tools around user identity verification, X.509 certificate/private key creation/issuance, and authentication/authorization management.
4. Increase network participation and adoption by providing a wide variety of secure on-ramps and by making technological complexity transparent to the end user.

Based on these principles and with several years of refinement, VisionShare has built an Internet-based PKI-secured healthcare data network utilized by over 3000 hospitals and over 16,000 total sites. Large hospitals typically use VisionShare server appliances as their secure gateways to trading partners. Distributed entities or small clinics often choose our X.509 client certificate authenticated web portal as a simple way to participate. Practice management or electronic medical record vendors choose an X.509 client certificate authenticated REST-based Secure Exchange API (SEAPI) as their secure on-ramp. REST stands for REpresentational State Transfer and is a lightweight approach to programmatically interfacing with the

2829 University Ave SE Suite 800
Minneapolis, MN 55414
w: www.visionshareinc.com
p: 612.460.4301
f: 612.460.4343

VisionShare network. Of course to be compliant with the P.A.I.N. principle, the REST-based SEAPI uses X.509 client-certificate authenticated TLS (Transport Layer Security) sessions.

Security

All communication within the VisionShare network requires the use of X.509 client and server certificates and associated private keys regardless of whether the client environment is a web browser, VisionShare server, or a SEAPI-enabled medical record system. In all cases, the TLS handshake protocol is used to provide client and server authentication. Once the TLS handshake is complete, the VisionShare server software can utilize unique names within the X.509 client certificate to authorize access to services and write audit log entries. Persistent messages are PKI signed using an underlying SHA-256 hash function, and PKI encrypted using an underlying AES-256 symmetric encryption algorithm.

Identity Verification

The VisionShare network is secured by X.509 certificates and private keys issued by a tightly controlled VisionShare Certificate Authority called Neutralus. Without exception, every user of a VisionShare X.509 certificate and private key has completed a stringent identity verification process which includes the presentation of a valid government issued picture ID. Through years of careful refinement, VisionShare has also created a scalable and secure certificate generation and distribution process. If a user is diligent in completing his portion of the process, he can be up and running on the VisionShare network in a matter of hours. Supporting the business processes is a set of infrastructure tools that enables the efficient management of trading partner authorization and network monitoring.

Addressability and Routability

Each Neutralus certificate contains a unique user identifier in the Subject Distinguished Name that serves as the user's address on the VisionShare network. Nodes on the VisionShare network maintain a distributed map of routing information that is used, after appropriate authentication and authorization, to send the data directly to the recipient node.

Practicality and Simplicity of Integration

Reducing complexity for users and integrating with installed systems accelerates adoption of healthcare data exchange. For example, the REST-based VisionShare SEAPI provides a simple and practical secure on-ramp for healthcare messaging. While REST may not inherently provide message-level security mechanisms to ensure privacy, integrity, and non-repudiation, the

2829 University Ave SE Suite 800
Minneapolis, MN 55414
w: www.visionshareinc.com
p: 612.460.4301
f: 612.460.4343

VisionShare approach combines REST with PKI signatures and encryption of persistent messages thereby addressing this concern. This combination gives the healthcare entity the option of a much simpler interface into the healthcare message exchange network while maintaining message privacy, integrity, and non-repudiation. Through years of experience, VisionShare has built an understanding of how much complexity each segment of the healthcare market can handle. Using a pluggable software architecture, VisionShare can securely tailor the interface for various types of users resulting in quicker adoption of new innovations through protocol bridging.

VisionShare and the Direct Project

High-Level Comparison

The architecture and implementation of the VisionShare network is strikingly similar to the Direct Project. From a provider point of view, a VisionShare server (hosted or locally installed) plays the role of a Health Information Service Provider (HISP) in the context of the VisionShare network. In other words, it handles PKI security, presents a wide variety of secure edge protocols, routes messages, and simplifies the experience of secure data exchange. In a nutshell, it meets the provider where he is at today, and enables rational evolution to the exchange needs of tomorrow.

Security

To achieve end-to-end privacy, authentication, message integrity, and non-repudiation, the Direct Project specifies payload signing and encryption through X.509 certificates combined with the S/MIME standard. The VisionShare platform also employs X.509 certificates for both payload PKI operations and TLS-based machine-to-machine authentication and authorization. The S/MIME standard has been employed within the VisionShare product line for years. When a message arrives at its destination within the VisionShare network, the principles of PKI signatures and encryption ensure that it came from the advertised party and could not be seen by anyone other than the intended receiver.

Certificate Management

The Direct Project has served as an excellent venue for the discussion and trial of techniques and policies surrounding the management and distribution of private keys and X.509 certificates. The VisionShare Direct HISP has successfully interoperated with other HISPs using production DNS as a readily available, scalable, and proven certificate directory. The VisionShare network has primarily used the Neutralus CA mentioned earlier. In certain

2829 University Ave SE Suite 800
Minneapolis, MN 55414
w: www.visionshareinc.com
p: 612.460.4301
f: 612.460.4343

controlled situations, certificates issued from third party Certificate Authorities have been allowed on the edge of the VisionShare network, but only after the policies and procedures of the third party CA were carefully scrutinized. The Direct Project allows a more diverse CA environment which, we believe, will foster innovation and improve secure communication if done within a clear set of policy guidelines. As mentioned earlier, proper identity verification is a critical link in the chain of trust that VisionShare has created and that the Direct Project will create over time.

Backbone Protocol

The required Direct Project backbone protocol (in other words, the HISP-to-HISP protocol) is SMTP. The VisionShare network has mostly utilized client-certificate authenticated HTTPS as the backbone protocol. In the context of a payload-based security infrastructure such as S/MIME, the specific protocol used on the backbone lessens in importance. What the Direct Project has done correctly is choose a ubiquitous and well-known backbone protocol in SMTP, thereby lowering the barrier to HISP participation. This was clearly demonstrated, we believe, at the Direct Project connect-a-thon in San Francisco last month.

Edge Protocols

A Direct Project edge protocol is the secure communication mechanism used by providers to communicate with their HISP. In Direct today, this is typically represented as an email client speaking SMTP/POP3/IMAP over TLS to its HISP. Much of the flexibility and ease of use that is inherent in the VisionShare network emanates from the wide variety of secure edge protocols and deployment options that providers can use to speak to their VisionShare server. It is the existence of the edge protocol concept in both the VisionShare network and the Direct Project that allows providers to securely communicate today using protocols that leverage existing investments of time and money. For example, in the current VisionShare network, a provider may use sFTP to securely communicate with a resident VisionShare server. The VisionShare server PKI signs and encrypts the data and, using the backbone protocol discussed earlier, routes the message to the destination VisionShare server. The destination server PKI decrypts and verifies the message and delivers it to the receiver using a secure edge protocol with which the receiver is comfortable (for example, HTTP/S). The Direct Project architecture is conceptually identical with small variations in protocol choices. The end result is provider-to-provider secure communication that meets each provider where it is at technologically while simultaneously insulating each side from the protocol details of the other.

2829 University Ave SE Suite 800
Minneapolis, MN 55414
w: www.visionshareinc.com
p: 612.460.4301
f: 612.460.4343

The VisionShare Direct Project public health pilot initiatives are meeting public health departments where they are at today by securely utilizing PHINMS as an edge protocol. The provider side of the communication can choose from other secure protocols such as HTTPS/REST and do not need to understand the details of PHINMS. Both sides now have the freedom to evolve their communications architecture internally without affecting trading partners.

Receipt Confirmation

The Direct Project specifies the Message Disposition Notification (MDN) email message as a mechanism for sending confirmation of receipt. It remains to be seen how fully this will be adopted. The VisionShare network treats receipts as an application level function and does not have built-in receipt confirmation. Rarely have we heard the request for such a function to be built into the communication layer. Many existing workflows have application level receipts built into them (for example, the X12 997 functional acknowledgement).

We are excited to see the Direct Project architecture match the VisionShare network architecture so closely. The approach has worked well for us for over 10 years and we are confident that it will scale well as the Direct Project moves from pilot to production.

VisionShare and CONNECT

VisionShare first began working with the CONNECT software when version 2.0 was released in early Spring of 2009. We modeled CONNECT as an edge protocol on the VisionShare network and ran experiments to understand its capabilities. Currently we are engaged in deploying a CONNECT gateway as part of the CMS esMD initiative. VisionShare customers will use the existing VisionShare network to securely transmit medical documentation to the VisionShare CONNECT gateway, which will relay the information into the CMS gateway. The CONNECT-oriented link into CMS is modeled as an edge protocol on the VisionShare network. We envision the Direct Project integrating into CONNECT-based network in a similar manner. In an interesting twist, we are weighing the pros and cons of presenting the esMD endpoint to providers as a Direct Project address and securely transmitting esMD data over a Direct Project network.

2829 University Ave SE Suite 800
Minneapolis, MN 55414
w: www.visionshareinc.com
p: 612.460.4301
f: 612.460.4343

Looking Back

After ten years of experience moving health care data in a PKI secured network, we are proud of our accomplishments. We have proven that PKI processes and technologies can be deployed on a wide scale successfully. We have proven that the high level architecture on which the VisionShare network is built is reliable, scalable, and meets the needs of providers where they are at today. We have a 94% customer renewal rate from year to year with much of the 6% loss coming from expected mergers and acquisitions in the provider space. Our customers are insulated from their trading partners' technological choices and sincerely appreciate the value that such insulation provides.

However, there are areas in which challenges remain. We know that semantic interoperability is a challenge for our customers. While it is a giant leap forward to provide a secure communications fabric that insulates trading partners from one another at the protocol level, that same leap needs to occur at the payload level. When a receiver can accept an HL7 message but a sender cannot produce it, there is a semantic gap that providers need filled.

We also recognize that the opening up of the addressing, routing, and security mechanisms used within the VisionShare network will be critical moving forward. The Direct Project has been instrumental in moving forward the dialog around addressing, routing, and security interoperability for directed exchange.

Looking Forward

We at VisionShare have worked hard over the past ten years to learn what works and what does not in the arena of directed secure healthcare exchange. We believe the following are critical requirements to successfully execute the next phase in interoperable and secure nationwide healthcare exchange.

1. Never compromise on ensuring privacy, authentication, message integrity, and message non-repudiation within the communications fabric. Place PKI technology and process at the center of your efforts and maintain consistent policy and process for identity verification. Clearly state and enforce requirements for securing data at-rest.

2829 University Ave SE Suite 800
Minneapolis, MN 55414
w: www.visionshareinc.com
p: 612.460.4301
f: 612.460.4343

2. Create standards for directed exchange around endpoint addressability, security, and message routing. The Direct Project is well on its way to achieving this.

3. Always enable simple but secure on-ramps that hide complexity from the provider but ensure security. The Direct Project is on the right track by explicitly calling out the concepts of edge protocols and HISPs.

4. Do everything reasonable to meet providers technologically where they are at today. Allow them to evolve over time but still gain significant benefits now.

5. Where possible, help solve the problem of semantic interoperability.

We believe the Direct Project has gone a long way towards meeting these requirements. VisionShare is excited to continue our support.

Thank you for your time today.

2829 University Ave SE Suite 800
Minneapolis, MN 55414
w: www.visionshareinc.com
p: 612.460.4301
f: 612.460.4343